Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the application.

Listing of Claims:

1. (Currently amended) An apparatus for transmitting a file through a network, the apparatus comprising:

a file-splitting processor ~~that~~ for splitting[[s]] a file into a plurality of message segments and assigning one of a plurality of destination addresses to each segment, the plurality of ~~message segments to a plurality of~~ destination addresses being assigned to a receiving host; and

a message segment transmitter for transmitting the plurality of message segments to the receiving host using the plurality of destination addresses.

2. (Currently amended) The apparatus of claim 1 wherein the file-splitting processor further comprises a file converter ~~that~~ for convert[[s]]ing the file into N message segments such that ~~enable reassembly of~~ the file is reassemblable from a subset of any K of the message segments at the receiving host, ~~wherein~~ N and K ~~are~~ being positive integers[[,]] and N >K >1.

3. (Currently amended) The apparatus of claim 1 wherein the file-splitting processor is configured for ~~further~~ assign[[s]]ing one of a plurality of source addresses to each of the plurality of message segments, thereby ~~to~~ imped[[e]]ing ~~unauthorized~~ attempts to ~~observe~~ ascertain the ~~true~~ source of [[a]] the ~~transmitted~~ file.

4. (Currently amended) The apparatus of claim 1, further comprising a message segment monitor for detecting non-receipt of ~~at least one of a second plurality of~~ a subset of the plurality of message segments ~~transmitted to the apparatus~~.

5. (Currently amended) The apparatus of claim 1, further comprising an address allocator for assigning ~~and reassigning N~~ a subset of the plurality of destination addresses to the receiving host.

6. (Currently amended) An apparatus for transmitting a file through a network, the apparatus comprising:

a file-splitting processor ~~that~~ for split[[s]]ting the file into a plurality of message segments and assign[[s]]ing one of a plurality of source addresses to each message segment of the plurality of message segments, thereby ~~to~~ disguis[[e]]ing the origin of the file; and

a message segment transmitter for transmitting the plurality of message segments to a receiving host.

7. (Currently amended) The apparatus of claim 6 wherein the file-splitting processor is configured for ~~further~~ assigning one of a ~~addresses the plurality of message segments to a~~ plurality of destination addresses assigned to the receiving host to each message segment of the plurality of message segments.

8. (Currently amended) A method ~~of~~ for securely transmi~~ssion~~tting ~~of~~ a file through a network, the method comprising:

(a) at a source host, splitting the file into a plurality of message segments;

(b) addressing, at the source host, each message segment of the plurality of message segments ~~to~~ using one of a plurality of destination addresses assigned to a receiving host; and

(c) transmitting the plurality of message segments to the receiving host with the plurality of destination addresses.

9. (Currently amended) The method of claim 8 wherein the plurality of message segments are addressed ~~addressing comprises addressing the plurality of message segments~~ in one-to-one correspondence to at least a ~~portion~~ subset of the plurality of destination addresses.

10. (Currently amended) The method claim 8 wherein splitting the file into a plurality of message segments comprises converting the file into N message segments such that ~~enable reassembly of~~ the file is reassemblable from a subset of any K of the message segments, ~~where~~ N and K ~~are~~ being positive integers[,] and N >K >1.

11. (Currently amended) The method of claim 10, further comprising [[(d)]] assigning N destination addresses to the receiving host, ~~and~~ wherein the ~~step of addressing comprises addressing the~~ N message segments are addressed using one of ~~to~~ the N destination addresses assigned to the receiving host.

12. (Currently amended) The method of claim 11, further comprising causing the receiving host to cease receiving messages ~~via~~ on at least one of the N destination addresses in response to ~~upon detection of~~ an attack on the at least one of the destination addresses.

13. (Currently amended) The method of claim 12 wherein the receiving host ~~is permitted to~~ ceases to receive ~~ing~~ messages via no more than (N-K) destination addresses, thereby ~~ensuring~~ facilitating reassembly of the file by the host.

14. (Currently amended) The method of claim 11, further comprising:

(e) reassembling the N message segments into a reassembled file at the receiving host;

(f) ~~causing the receiving host to~~ splitting [[a]] the reassembled file into a second set of N message segments at the receiving host; and

~~(f)~~(g) ~~causing the receiving host to~~ transmitting the second set of N message segments from the receiving host using the N destination addresses.

15. (Currently amended) The method of claim 8, further comprising :

(d) ~~causing the receiving host to~~ retransmitting the plurality of message segments from the receiving host.

16. (Currently Amended) The method of claim 15 wherein retransmitting the plurality of message segments from the receiving host ~~the step of causing the receiving host to retransmit~~ comprises ~~causing the receiving host to~~ retransmitting the plurality of message segments to at least two of a plurality of intermediate hosts, ~~to~~ thereby relaying the plurality of message segments along more than one path through the network.

17. (Currently amended) The method of claim 8, further comprising:

(d) selecting ~~as~~ a virtual network comprising a plurality of hosts, the plurality of hosts ~~that~~ includinges the receiving host; ~~and~~

(e) assigning each ~~one~~ host of the plurality of hosts to ~~one~~ a domain of a plurality of domains;[[, and]]

(f) designating sets of the host pairs, each host pair comprising two hosts assigned to the same domain or a neighboring domain; and

(g) ~~wherein the step of transmitting comprises permitting~~ constraining travel of each message segment ~~one~~ of the plurality of message segments ~~to travel~~ to the receiving host ~~only~~ via relays between host pairs~~, each one of the host pairs selected from one of a same domain and a neighboring domain~~.

18. (Currently amended) The method of claim 8, further comprising:

(d) assigning a source address selected from a plurality of source addresses to each message segment of the plurality of message segments, thereby ~~to~~ imped[[e]]ing ~~unauthorized~~ attempts to ~~observe a true~~ ascertain the source of [[a]] the ~~transmitted~~ file.

19. (Currently amended) The method of claim 8, further comprising ~~causing the receiving host to~~:

(d) receiv[[e]]ing, at the receiving host, at least a portion of the plurality of message segments;

(e) reassembl[[e]]ing the file from the received message segments at the receiving host;

(f) splitting the reassembled file into a second plurality of message segments at the receiving host; and

(g) transmitting the second plurality of message segments from the receiving host.

20. (Currently amended) The method of claim 8 wherein step (c) ~~transmitting~~ comprises transmitting the plurality of message segments to at least one of an intermediate host and a destination host.

21. (Currently amended) The method of claim 8 wherein step (c) ~~transmitting~~ comprises transmitting from at least one of a source host and an intermediate host.

22. (Currently amended) The method of claim 8, further comprising:

(d) ~~causing the receiving host to~~ monitoring non-receipt by the receiving host of at least one of the plurality of message segments ~~to detect tampering with message segment transmission~~.

23. (Currently amended) The method of claim 8, further comprising:

(d) allocating M destination addresses for assignment to the receiving host;

(e) assigning N destination addresses of the M allocated destination addresses, where N is less than or equal to M; ~~to the receiving host~~ and

(e) ~~repeatedly changing~~ periodically reassigning to the receiving host at least a portion of the N destination addresses.

24. (Currently amended) The method of claim 10, further comprising:

(d) ~~repeatedly changing~~ periodically reassigning at least a ~~portion~~ subset of the plurality of destination addresses assigned to the receiving host while leaving at least K of the destination addresses unchanged thereby permitting continuous receipt of messages by the receiving host, and

(e) notifying at least a portion of the network of the ~~changed~~ reassigned destination addresses~~, and wherein the step of addressing comprises addressing the plurality of message segments to at least the K unchanged addresses to permit continuous receipt of messages by the receiving host~~.

25. (Currently amended) The method of claim 8, further comprising:

(d) ~~causing a sending host to~~ adding status information associated with a sending host ~~concerning itself~~ to the message segment; and

(e) ~~causing the receiving host to~~ upon receipt by the receiving host, interpreting the status information to detect tampering with message segment transmission.

26. (Currently amended) The method of claim 8, further comprising:

(d) encoding the file to produce an encoded bit file having encoded bits, and

(e) scrambling the encoded bits, ~~and wherein the step of splitting the file splits~~ such that the encoded bit file is split into a plurality of message segments.

27. (Currently amended) A method of securely transmitting ~~ssion of~~ a file through a network, the method comprising:

(a) splitting the file into a plurality of message segments at a source host;

(b) at the source host, assigning one source address of a plurality of source addresses to each message segment of the plurality of message segments, thereby ~~to~~ disguise[[e]]ing the origin of the file; and

(c) transmitting the plurality of message segments.

28. (Currently amended) The method of claim 27, further comprising:

(d) assigning one destination address of a plurality of destination ~~addressing the plurality of message segments to a plurality of~~ addresses assigned to a receiving host to each message segment of the plurality of message segments.

29. (Currently amended) A method ~~of~~ for securely transmitting ~~ssion of~~ a ~~message~~ file through a network, the method comprising:

(a) splitting the file into a plurality of message segments, each message segment comprising a destination specifier, encrypted protocol information, and encrypted message data~~, the protocol information and message data being encrypted~~;

(b) ~~causing~~ receiving a message segment ~~to be received by~~ at a receiving host;

(c) ~~causing the receiving host to~~ decrypting the message data ~~routing information~~ to determine a ~~downstream~~ destination host;

(d) ~~causing the receiving host to~~ encrypting the ~~routing information and~~ message data in accordance with an encryption protocol accessible to the destination host;

~~(e), and to~~ (e) transmitting the [[thus-]]encrypted message segment to the destination host; and

~~(e)~~ (f) repeating steps (a)-(~~d~~e) for other message segments, ~~to~~ thereby facilitat[[e]]ing recovery of the message by ~~an ultimate~~ the destination host.

30. (Currently amended) The method of claim 29 wherein the message segment has a length, and further comprising ~~causing the receiving host to~~ altering the length.

31. (Currently amended) The method of claim 29 ~~further comprising causing~~ wherein the receiving host ~~to negotiate with~~ and the destination host negotiate to determine the encryption protocol.

32. (Currently amended) The method of claim 29, further comprising causing the receiving host to adding status information concerning the receiving host ~~itself~~ to the message segment, and, ~~causing~~ at the receiving host, ~~to~~ interpreting the status information to detect tampering with message segment transmission.

33. (Currently amended) A method ~~of~~ for defining and operating a network topology to camouflage network traffic patterns and volume, the network comprising a plurality of hosts, the method comprising:

(a) assigning each ~~one~~ host of ~~the~~ a plurality of hosts to ~~one~~ a first domain of a plurality of domains; and

(b) ~~permitting~~ restricting network traffic to message transmissions ~~from each host to~~ among hosts within the same domain ~~of the host~~ or a neighboring domains ~~that neighbors the domain of the host~~, thereby defining multiple redundant relay paths among hosts, thereby ~~; and~~

~~(c) distributing traffic across the network, thereby~~ camouflaging message sources and destinations.

34. (Currently amended) The method of claim 33, further comprising:

(~~d~~c) reassigning at least one host of the plurality of the hosts to a second domain ~~different one~~ of the plurality of domains, thereby changing network traffic patterns.

35. (Currently amended) The method of claim 33, further comprising:

(d) assigning [[a]] one of a plurality of addresses selected from a pool of addresses ~~to~~ with each one of the plurality of hosts;

(e) reassigning at least one of the plurality of assigned addresses from [[a]] the pool of addresses; and

(f) notifying the plurality of hosts of the reassigned ~~plurality of~~ addresses.

36. (Currently amended) The method of claim 35 wherein ~~the step of reassigning comprises reassigning only~~ a portion of the plurality of addresses is reassigned at any one time to permit the use of ~~a remaining unreassigned portion of the plurality of addresses~~ addresses not having been reassigned ~~while~~ for notifying the plurality of hosts of the ~~reassigned~~ reassigned ~~plurality of~~ addresses.